ELSEVIER

Discrete Mathematics 162 (1996) 49–66

DISCRETE MATHEMATICS

On a class of finite upper half-planes

Mihai Caragiu

Department of Mathematics, Pennsylvania State University at University Park and Institute of Mathematics, Bucharest*

Received 17 July 1995

Abstract

Using an exponential sum associated to the Legendre character, we introduce a finite 'upper half-plane' $V(q)$, by defining a metric on the set given by the union between the quotient of $F_{q^2} - F_q$ with respect to the Frobenius action, and an extra point ∞, which appears as a collapse of the field F_q. We also introduce, for every odd prime power q, the 'length spectrum' $\sum_q$, that is, the set of all possible distances between distinct points of $V(q)$, which plays the role of a 'parameter space' for a class of associated graphs $V(q;k)$, $k \in \sum_q$, for which the 'finite parts' $V_0(q;k)$ are regular. Up to a normalization, the whole metric space $V(q)$ can be seen as a small perturbation of a complete graph with $1 + (q^2 - q)/2$ vertices.

Finally, we show how these results generalize to any higher dimension n. The corresponding metric space $V_n(q)$ is obtained out of the set of the orbits of the Frobenius action on F_{q^n} over F_q, by making appropriate identifications.

1. Introduction

The classical upper half-plane is defined by $H = \{z \in C | \mathrm{Im}(z) > 0\}$, or $H = (Z/2Z)\backslash(C - R)$, where $Z/2Z$ acts by complex conjugation. H is endowed in a natural way with a metric (Poincaré) $ds = |dz|/y$, and represents the universal covering for each compact Riemann surface of genus at least 2.

In a series of papers [1, 4, 2], a finite analogue of H is considered, by taking the finite field F_q, q odd, instead of the real field R. The finite upper half-plane is defined by

$$H_q = \{z = x + y\sqrt{w} \mid x, y \in F_q, y \neq 0\} \tag{1}$$

where $w \in F_q$ is a nonsquare (note that $\sqrt{w}$ plays the role of $i = \sqrt{-1}$ in the Poincaré's upper half-plane). The group $G = GL(2, q)$ (even $SL(2, q)$) acts transitively on H_q, by $gz = (az + b)/(cz + d)$, where the element g is given by $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. The

* Corresponding address: E-mail: caragiu@math.psu.edu.

SSDI 0012-365X(95)00236-7

analogue of the Poincaré metric is given as a point-pair invariant, i.e., a map $d: \boldsymbol{H}_q \times \boldsymbol{H}_q \to \boldsymbol{F}_q$, such that $d(gz, gt) = d(z, t)$ for all $g \in G$ and $z, t \in \boldsymbol{H}_q$. More precisely, d is defined as

$$d(z,t) = \frac{N(z-t)}{\mathrm{Im}(z)\mathrm{Im}(t)}, \tag{2}$$

where $N(z) = z\bar{z} = z^{1+q}$ is the usual norm from $\boldsymbol{F}_{q^2}$ to $\boldsymbol{F}_q$, and $\mathrm{Im}(z)$, in this case, is defined to be y whenever $z = x + y\sqrt{w}, x, y \in \boldsymbol{F}_q$. A number of interesting results are derived, especially concerning a class of eigenfunctions of the Laplacians of the graphs associated to the upper half-planes, spherical Fourier transforms and Selberg trace formula.

Our aim will be to try to define a class of 'finite upper half-planes' endowed with usual (i.e., real-valued) metrics. In constructing such metrics we make use of a character sum associated with the quadratic character χ of $\boldsymbol{F}_{q^2}$, in which the range of summation is $\boldsymbol{F}_q$. This type of sums is by no means new: similar sums were considered earlier by Davenport [5]. He shows, for example, that if θ is any element generating the finite field $\boldsymbol{F}_{p^k}$ over its prime subfield $\boldsymbol{F}_q$, then

$$\sum_{a=0}^{p-1} \chi(\theta + a) = \mathrm{O}(p^{(2k+1)/(2k+2)}).$$

If fact, Weil's Theorem [3, 5, 12, 8] shows that the right-hand side of the above estimate can be sharpened to $\mathrm{O}(\sqrt{p})$.

In the series of papers [1, 4, 2], some regular Ramanujan graphs are associated to the finite upper half-plane (1) endowed with the point-pair invariant (2). Namely, if w in (1) is a primitive root g of $\boldsymbol{F}_q$, and if $a \in \boldsymbol{F}_q \setminus \{0, 4g\}$, then a graph $X_q(g, a)$ is constructed by drawing an edge between z and t whenever $d(z, t) = a$, d being given by (2). One may show [1] that $X_3(-1, 1)$ is the octahedron, while the three graphs for $q = 5$ can be placed on the dodecahedron. The degree of every vertex of $X_q(g, a)$ is $q + 1$.

Our construction is based on the real-valued metric (to be more precise, all its values are integers) induced by the pseudometric (3) (see Section 2). This pseudometric forces us to identify every element $z \in \boldsymbol{F}_{q^2}$ with $\bar{z}$, where $\bar{z}$ represents the action of the Frobenius automorphism $\bar{z} = z^q$. Also, the elements of $\boldsymbol{F}_q$ will collapse to a single point ∞, 'the point at infinity'. At least formally, the finite structure $V(q)$ we obtain resembles an 'upper half-plane'. Some specific problems appear whenever one considers such an analogy. For example, if we fix any $k \in \{1, 2, \ldots, q\}$, one may define a graph $V(q; k)$, say, by drawing an edge between any two points at a distance k. While in [1, 4, 2], all the graphs $X_q(g, a)$ are nonempty, in our case the problem of estimating the range of the distance function (which we shall call 'length spectrum', see Section 5 is different. Moreover, we will see that the 'finite parts' $V_0(q; k)'s$ (obtained out of $V(q; k)$ by deleting the point at infinity together with all the incident edges), if nonempty, follow to be regular.

In Section 2 we state the main results needed for the construction of the finite upper half-planes $V(q)$. The proofs are actually given in Section 3. We follow, in fact, two alternative ways or 'philosophies'. The first one is that of algebraic geometry. It provides us with a quick proof based on the celebrated result of Hasse [7] about the number of rational points on elliptic curves over finite fields. The second approach is based on character sums, which will prove to be very effective in our attempt to generalize the whole theory to higher dimensions, which will be pursued in Section 6.

Explicit presentations of $V(3)$ and $V(5)$ are offered in Section 4.

In Section 5 we introduce, for every odd prime power q, a class of associated graphs $V(q;k)$, $k \in \sum_q$, where $\sum_q$ is the 'length spectrum' of $V(q)$, that is, the set of all possible distances between distinct points of $V(q)$. The 'finite part' $V_0(q;k)$ of every $V(q;k)$ proves to be regular. In the same section we prove an asymptotic estimate of the length spectrum, according to which, if q is large, the elements of $\sum_q$ can be evaluated as $q/2 + O(\sqrt{q})$: this is just another way in which one can 'taste' the *Riemann Hypothesis* for algebraic curves over finite fields, proved by Weil [12] in 1948.

In Section 6, by using the powerful Weil estimates for character sums (see [8, Ch. 5] for a detailed account), we prove that the 'plane construction' can be extended to any higher dimension n, provided if q is large enough (more precisely, if $q > (2n-1)^2$). The corresponding metric spaces $V_n(q)$, $n \geqslant 2$, are constructed by making appropriate identifications in the orbit space of the Frobenius action on $\boldsymbol{F}_{q^n}/\boldsymbol{F}_q$.

2. The metric

Let q be an odd prime power. We may choose $\boldsymbol{j}$ in $\boldsymbol{F}_{q^2}$ with $\boldsymbol{F}_{q^2} = \boldsymbol{F}_q(\boldsymbol{j})$ and a minimal equation over $\boldsymbol{F}_q$ of the form $\boldsymbol{j}^2 = t$, where $t \in \boldsymbol{F}_q^* - (\boldsymbol{F}_q^*)^2$.

Let $\chi : \boldsymbol{F}_{q^2}^* \to \{-1, 1\}$ be the quadratic (Legendre) character. It is obvious that the restriction of χ to $\boldsymbol{F}_q^*$ is trivial, every element of $\boldsymbol{F}_q$ being a square in $\boldsymbol{F}_{q^2}$. For this reason we will extend χ to $\boldsymbol{F}_{q^2}$ in a quite unusual way, by taking $\chi(0) := 1$.

We are now able to give the definition of a real function $d : \boldsymbol{F}_{q^2} \times \boldsymbol{F}_{q^2} \to \boldsymbol{R}$, which will lead us to the metric on our finite upper half-plane:

$$d(x, y) = \frac{1}{2} \sum_{a \in \boldsymbol{F}_q} |\chi(x + a) - \chi(y + a)|. \tag{3}$$

With a single exception, d satisfies the usual metric axioms, namely $d(x, y) = 0$ does not imply $x = y$ (that is, d is a *pseudometric*). For example, $d(x, y) = 0$ for $x, y \in \boldsymbol{F}_q$. Moreover, it is easy to see that for every z in $\boldsymbol{F}_{q^2}$, we have

$$d(z, \bar{z}) = 0. \tag{4}$$

(If $z = a + b\boldsymbol{j}$, $a, b \in \boldsymbol{F}_q$, we denote the action of Frobenius by $\bar{z} = a - b\boldsymbol{j} = z^q$, representing the analogue of the classical complex conjugation.)

We say that two elements $x, y \in \boldsymbol{F}_{q^2}$ are *equivalent* if $d(x,y) = 0$, or, which is the same, if

$$\chi(x + a) = \chi(y + a) \quad \forall a \in \boldsymbol{F}_q.$$

Let us denote the fact that x and y are equivalent by $x \sim y$. If we consider the factor set, then the elements of $\boldsymbol{F}_q$ collapse to a single point, which we shall denote by ∞. Moreover, two basic results hold:

Proposition 1. *If $x \in \boldsymbol{H}_q$ and if $y \in \boldsymbol{F}_q$, then $x \not\sim y$.*

Proposition 2. *For every $x, y \in \boldsymbol{H}_q$, $x \sim y$ if and only if $y = \bar{x}$ or $y = x$.*

Stated in another way, it follows that if $\hat{\boldsymbol{H}}_q$ is the quotient of $\boldsymbol{H}_q$ by the action of the Frobenius automorphism $z \mapsto \bar{z}$, then the metric space induced by our pseudometric $d: \boldsymbol{F}_{q^2} \times \boldsymbol{F}_{q^2} \to \boldsymbol{R}$ is

$$\boldsymbol{V}(q) := \hat{\boldsymbol{H}}_q \cup \{\infty\}.$$

Thus, at least formally, we have restored a familiar structure, namely an 'upper half-plane' together with its point at infinity (recall that the point at infinity in the complex case represents a collapse of the set of all cusps — $\boldsymbol{Q} \cup \{\infty\}$ — which are equivalent by the action of $\boldsymbol{SL}(2, \boldsymbol{Z})$).

Note that whenever $a, b \in \{-1, 1\}$ we have the obvious identity

$$|a - b| = 1 - ab.$$

By using the above relation, one easily sees that the function d given by (3) can also be expressed as

$$d(x,y) = \frac{1}{2}\left[q - \sum_{a \in \boldsymbol{F}_q} \chi((x + a)(y + a)) \right]. \tag{5}$$

One may remark the similarity between (5) and the exponential sums considered by Davenport (see Section 1). Obviously, the range of the d-function is contained in $\{0, 1, \ldots, q\}$.

3. The proofs

First we must note that the following relations

$$d(x,y) = d(x + a, y + a), \tag{6}$$

$$d(x,y) = d(ax, ay), \tag{7}$$

$$d(x,y) = d(\bar{x}, \bar{y}), \tag{8}$$

hold for every $x, y \in \boldsymbol{F}_{q^2}$ and every $a \in \boldsymbol{F}_q$.

They follow easily, by definition. For example, we have

$$2d(\bar{x}, \bar{y}) = \sum_{a \in \boldsymbol{F}_q} |\chi(x^q + a) - \chi(y^q + a)|$$

$$= \sum_{a \in \boldsymbol{F}_q} |\chi((x + a)^q) - \chi((y + a)^q)|$$

$$= \sum_{a \in \boldsymbol{F}_q} |\chi(x + a) - \chi(y + a)| = 2d(x, y).$$

Note that here we use the fact that q is odd.

Now, suppose that Proposition 1 is not true. Then, using transformations of types (6) and (7), affine over $\boldsymbol{F}_q$, we may suppose that $d(\boldsymbol{j} + a, 0) = 0$ for some $a \in \boldsymbol{F}_q$. That means that $\chi(\boldsymbol{j} + a + c) = \chi(c) = 1$ for every $c \in \boldsymbol{F}_q$. In particular, it follows that $\boldsymbol{j} + d$ is a square in $\boldsymbol{F}_{q^2}$ for each $d \in \boldsymbol{F}_q$. But then, because the elements of $\boldsymbol{F}_q$ are themselves squares, every element in $\boldsymbol{F}_{q^2}$ has to be a square, which is an obvious contradiction; Proposition 1 is proved.

Before starting the proof of Proposition 2, let us denote by ψ the quadratic character of $\boldsymbol{F}_q$. It is a well-known fact that the relation between ψ and its 'lifting' χ is given by

$$\chi(z) = \psi(Nz) \tag{9}$$

for every $z \in \boldsymbol{F}_{q^2}^*$, where $Nz = z\bar{z} = z^{1+q}$ is the usual norm map from $\boldsymbol{F}_{q^2}$ to $\boldsymbol{F}_q$ (indeed one has $\chi(z) = z^{(q^2-1)/2} = (z^{1+q})^{(q-1)/2} = \psi(Nz)$).

Let now $x, y \in \boldsymbol{H}_q = \boldsymbol{F}_{q^2} - \boldsymbol{F}_q$. It is easy to see that $x \sim y$ whenever $y = \bar{x}$. If, for example, $y = x^q$, then

$$\chi(x + a) = \chi((x + a)^q) = \chi(x^q + a) = \chi(y + a) \quad \forall a \in \boldsymbol{F}_q$$

However, the converse is not quite obvious. We need to prove that if $x, y \in \boldsymbol{H}_q$ satisfy

$$\chi(x + a) = \chi(y + a) \quad \forall a \in \boldsymbol{F}_q \tag{10}$$

then x and y are either equal or conjugate by the Frobenius action (i.e., $y = \bar{x}$).

By using (9), we can rewrite (10) as

$$\psi((x + a)(\bar{x} + a)) = \psi((y + a)(\bar{y} + a)) \quad \forall a \in \boldsymbol{F}_q$$

or, equivalently,

$$\psi[(x + a)(\bar{x} + a)(y + a)(\bar{y} + a)] = 1 \quad \forall a \in \boldsymbol{F}_q \tag{11}$$

So, all we need to do is to show that if (11) is true, then $y = x$ or $y = \bar{x}$.

At this point, one may follow either of two lines of argument, reflecting two deeply connected mathematical schools or '*philosophies*':

Algebraic geometry. More precisely, the algebraic geometry of curves over finite fields, or, equivalently, the theory of algebraic function fields of one variable over finite

constant fields (one may see [10] for a detailed approach in the function fields case). The main result in the field is the celebrated '*Riemann Hypothesis*' for curves over finite fields, first proved by Hasse [11] for elliptic curves, then in the general case by Weil [8]. We will actually use only the result of Hasse: the number N of $\boldsymbol{F}_q$ -rational points on a complete elliptic curve defined over $\boldsymbol{F}_q$ satisfy the inequality

$$|N-(q+1)| \leqslant 2\sqrt{q}.$$

Character sums. The theory of character sums with polynomial arguments (the so-called '*Weil sums*') has, as noted earlier, a long history (one may see [9, Chs. 5 and 6]). Here we will use only a very important result (see Theorem 1 below), estimating the complete character sums for the multiplicative characters of finite fields, with a polynomial argument.

Both of them solve our problem. Here we will follow both ways, not only because this gives a taste of the underlying unity, but also because the character sum approach will be extremely useful in our generalization of the 'plane construction' to higher dimensions (see Section 6 for details).

Remark 1. Let $x = u + \boldsymbol{j}v$, $y = w + \boldsymbol{j}s$ be two elements of $\boldsymbol{F}_{q^2}$, $u, v, w, s \in \boldsymbol{F}_q$. If we use (9) and (5), the expression for d as a character sum will be given by

$$d(x,y) = \frac{1}{2}\left[q - \sum_{a \in \boldsymbol{F}_q} \psi(((a+u)^2 - tv^2)((a+w)^2 - ts^2))\right]. \tag{12}$$

Let us suppose then, by contradiction, that $x, y \in \boldsymbol{H}_q$ satisfy $y \neq x, \bar{x}$. Then, the polynomial

$$P(X) = (X+x)(X+\bar{x})(X+y)(X+\bar{y})$$

is separable (i.e., it has distinct roots). Using (11), it follows that $P(a)$ is a square in $\boldsymbol{F}_q^*$ for every a in $\boldsymbol{F}_q$. In other words, the elliptic curve defined over $\boldsymbol{F}_q$ by the equation

$$Y^2 = P(X) \tag{13}$$

has $2q$ finite $\boldsymbol{F}_q$-rational points. One can see (13) in a standard way as a two-sheeted covering of $\boldsymbol{P}^1$, ramified in four finite places, corresponding to the 4 linear factors of $P(X)$. The place at infinity of $\boldsymbol{P}^1$ is not ramified, so our curve (13) has two more rational points 'at infinity', adding up to a total of $N = 2q + 2$ $\boldsymbol{F}_q$-rational points. Now, we only have to apply the fundamental result of Hasse $|N-(q+1)| \leqslant 2\sqrt{q}$, which in this case gives $q + 1 \leqslant 2\sqrt{q}$, or $q = 1$, an obvious contradiction. This concludes the proof of Proposition 2.

We will now follow an alternative proof based on character sums estimates.

The following result is well known [9, Ch. 5, Theorem 5.41].

Theorem 1 (Weil [12]). *Let ψ be a multiplicative character of $\boldsymbol{F}_q$ of order $m > 1$ and let $f \in \boldsymbol{F}_q[X]$ be a monic polynomial of positive degree that is not an mth power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\boldsymbol{F}_q$ and assume that $d \geqslant 2$. Then there exist complex numbers $\omega_1, \omega_2, \ldots, \omega_{d-1}$, with*

$$|\omega_1| = |\omega_2| = \cdots = |\omega_{d-1}| = \sqrt{q}$$

only depending on f and ψ, such that for any integer $s \geqslant 1$, if we denote by $\psi^{(s)}$ the lifting of ψ to $\boldsymbol{F}_{q^s}$ given by

$$\psi^{(s)}(x) := \psi(N_{\boldsymbol{F}_{q^s}/\boldsymbol{F}_q}(x)), \quad x \in \boldsymbol{F}_{q^s}$$

then we have the estimate

$$\sum_{\gamma \in \boldsymbol{F}_{q^s}} \psi^{(s)}(f(\gamma)) = -\omega_1^s - \omega_2^s - \cdots - \omega_{d-1}^s.$$

In particular,

$$\left| \sum_{\gamma \in \boldsymbol{F}_q} \psi(f(\gamma)) \right| \leqslant (d-1)\sqrt{q}.$$

Let us apply the Weil estimates to the case $m = 2$, ψ being the quadratic character of $\boldsymbol{F}_q$, and $f(X) = P(X)$. Assume again, by contradiction that $y \neq x$ and $y \neq \bar{x}$. Then, again $P(X)$ has $d = 4$ roots in its splitting field (which is $\boldsymbol{F}_{q^2}$, in this case). Because the values taken by ψ are 1 or -1, we see that (11) is equivalent to

$$\sum_{a \in \boldsymbol{F}_q} \psi(P(a)) = q.$$

By using Weil's Theorem we will obtain $q \leqslant 3\sqrt{q}$, which is false whenever $q \geqslant 11$. The verification of the four other cases corresponding to the odd values of q which are smaller than 11 (namely $q = 3, 5, 7, 9$) is quite straightforward and will not be pursued here (nevertheless we will present the cases $q = 3$ and $q = 5$ in the next section, while briefly discussing the case $q = 7$ in Section 5).

In a few words, Proposition 2 is true, and we obtain in this way a finite metric space

$$V(q) = \hat{\boldsymbol{H}}_q \cup \{\infty\}$$

with exactly $1 + (q^2 - q)/2$ points. This is our finite 'upper half-plane'. The metric induced on $V(q)$ by the pseudometric d can be described in a standard way: if $x, y \in \boldsymbol{F}_{q^2}$ are two elements representing $\alpha, \beta \in V(q)$, respectively, then, if we agree to denote by the letter 'Δ' the metric induced on $V(q)$, one has $\Delta(\alpha, \beta) := d(x, y)$.

4. Examples: $V(3)$ and $V(5)$

Let us consider the cases in which q is 3 or 5. In the first one, we can take j as one root of the equation $X^2 + 1 = 0$ over $\boldsymbol{F}_3$. The field $\boldsymbol{F}_9$ will have then a suitable 'matrix presentation'

$$\begin{pmatrix} j-1 & j & j+1 \\ -1 & 0 & 1 \\ -j-1 & -j & -j+1 \end{pmatrix}$$

while the corresponding matrix of the quadratic character is

$$\begin{pmatrix} - & + & - \\ + & + & + \\ - & + & - \end{pmatrix} \tag{14}$$

Our complete upper half-plane will have, in this case, the structure

$$V(3) = \{A, B, C, \infty\}, \tag{15}$$

where A is a collapse of $\{j+1, -j+1\}$, B is a collapse of $\{-j, j\}$, C is a collapse of $\{j-1, -j-1\}$, and, as already defined, ∞ is a collapse of $\boldsymbol{F}_3$.

It is easy to see that the metric space associated to the upper half-plane (15) has the structure of a tetrahedron (one may check the character chart (14) and see that all the mutual distances between distinct points are equal to 2).

Next we consider the case $q = 5$, which is slightly more intricate. Here we agree to take j with the minimal equation $j^2 = 2$ over $\boldsymbol{F}_5$. Then the similar matrix arrangement for $\boldsymbol{F}_{25}$ will be

$$\begin{pmatrix} 2j-2 & 2j-1 & 2j & 2j+1 & 2j+2 \\ j-2 & j-1 & j & j+1 & j+2 \\ -2 & -1 & 0 & 1 & 2 \\ -j-2 & -j-1 & -j & -j+1 & -j+2 \\ -2j-2 & -2j-1 & -2j & -2j+1 & -2j+2 \end{pmatrix}$$

together with the corresponding matrix of the quadratic character

$$\begin{pmatrix} + & - & - & - & + \\ - & + & - & + & - \\ + & + & + & + & + \\ - & + & - & + & - \\ + & - & - & - & + \end{pmatrix}$$

One may use the fact that

$$\chi(aj + b) = \psi((aj + b)(-aj + b)) = \psi(b^2 - 2a^2) = \left(\frac{b^2 - 2a^2}{5}\right)$$

for every $a, b \in \boldsymbol{F}_5$. $V(5)$ has 11 elements, namely the classes

$$\infty = A_0, A_1, \ldots, A_{10}$$

with representants

$$0, \boldsymbol{j}, 2\boldsymbol{j}, 1+\boldsymbol{j}, 1+2\boldsymbol{j}, 2+\boldsymbol{j}, 2+2\boldsymbol{j}, -2+\boldsymbol{j}, -2+2\boldsymbol{j}, -1+\boldsymbol{j}, -1+2\boldsymbol{j},$$

respectively.

The following array represents the distances $\Delta_{ef} = \Delta(A_e, A_f)$, $0 \leqslant e, f \leqslant 10$:

*	0	1	2	3	4	5	6	7	8	9	10
0	0	3	3	3	3	3	3	3	3	3	3
1	3	0	4	4	2	2	2	2	2	4	2
2	3	4	0	2	2	2	4	2	4	2	2
3	3	4	2	0	4	4	2	2	2	2	2
4	3	2	2	4	0	2	2	2	4	2	4
5	3	2	2	4	2	0	4	4	2	2	2
6	3	2	4	2	2	4	0	2	2	2	4
7	3	2	2	2	2	4	2	0	4	4	2
8	3	2	4	2	4	2	2	4	0	2	2
9	3	4	2	2	2	2	2	4	2	0	4
10	3	2	2	2	4	2	4	2	2	4	0

(17)

Here the rows and columns are labelled, and at the intersection between the eth row and fth column stands the distance Δ_{ef}. Let us consider for a moment the case $q = p$, with p an odd prime. Let $\boldsymbol{j}$ be a generator of $\boldsymbol{F}_{p^2}$ over $\boldsymbol{F}_p$, satisfying a minimal equation $\boldsymbol{j}^2 = t$ over $\boldsymbol{F}_p$, with $t \in \boldsymbol{F}_p$ a nonsquare (if $p \equiv 3 (\mathrm{mod}\, 4)$, one may choose $t = -1$).

The character chart can be easily done if one takes into account the relation (9). Indeed, it reduces to the computation of the quadratic symbol $\psi(\cdot) = (\frac{\cdot}{p})$ in $\boldsymbol{F}_p$:

$$\chi(a\boldsymbol{j} + b) = \left(\frac{b^2 - ta^2}{p}\right)$$

for every $a, b \in \boldsymbol{F}_p$. Now, if we use (12), we see that for every $\alpha, \beta \in \boldsymbol{V}(p)$, having representants $a\boldsymbol{j} + b$, $c\boldsymbol{j} + d \in \boldsymbol{F}_{p^2}$, respectively, the distance $\Delta(\alpha, \beta)$ in $\boldsymbol{V}(p)$ can be expressed as

$$\Delta(\alpha, \beta) = \frac{1}{2}\left[p - \sum_{x=0}^{p-1}\left(\frac{x^2 + 2bx + b^2 - ta^2}{p}\right)\left(\frac{x^2 + 2dx + d^2 - tc^2}{p}\right)\right].$$

This seems to make the case $q = p$ slightly more effective from a computational point of view than the case of an arbitrary odd power q.

5. Associating graphs to finite upper half-planes: The length spectrum

As in [2], we may define a set of graphs attached to our finite 'upper half-plane' $V(q)$. Namely, for every positive integer k,

$$k = 1, 2, \ldots, q,$$

we define the graph $V(q;k)$ which has the adjacency matrix,

$$(\delta(\Delta_{ef}, k))_{ef},$$

where δ is Kronecker's symbol.

In the case $q = 3$, for example, we have only one nonempty graph, namely $V(3;2)$, the regular tetrahedron. In the case $q = 5$, the combinatorics of the associated graphs, $V(5;2)$, $V(5;3)$ and $V(5;4)$ is much more interesting. $V(5;3)$ is a nice tree, star-shaped: $\infty = A_0$ has degree 10, while $A_1, \ldots, A_{10}$ have degree 1 each.

$V(5;2)$ and $V(5;4)$ are not trees. Both of them have A_0 as an isolated vertex. If we exclude A_0 in each case we obtain two connected regular graphs, say $V_0(5;2)$ and $V_0(5;4)$, respectively. The degree of every vertex of $V_0(5;2)$ is 6, that is $V_0(5;2)$ is 6-regular. A similar result is obtained for $V_0(5;4)$, for which the degree of every vertex is 3. Let $V_0(q;k)$ represent the graph obtained from $V(q;k)$ by deleting the point ∞ (of course, together with all its edges, if any). A good connection with [1] (in which, we recall, if a is not 0 or $4g$, then $X_q(g,a)$ is $(q+1)$-regular) will be given by the fact that our $V_0(q;k)$'s are indeed regular (possibly empty: here we agree that an empty graph is a particular case of regular graph, namely a 0-regular graph). For example, when $q = 7$, in which $\boldsymbol{F}_{49} = \boldsymbol{F}_7(\boldsymbol{j})$, with $\boldsymbol{j}$ satisfying the equation $\boldsymbol{j}^2 + 1 = 0$ over $\boldsymbol{F}_7$, one sees that $V_0(7;2)$ is 6-regular, $V_0(7;4)$ is 12-regular and $V_0(7;6)$ is 2-regular (I want to thank Professor Leonid Vaserstein, for helping me with a lot of computer searches). The proof of regularity is an easy consequence of the relations (6) and (7). Indeed, let us take an element $a\boldsymbol{j} + b \in \boldsymbol{H}_q$. Also let us fix $k \in \{1, 2, \ldots, q\}$. Then, (6) and (7) imply that there is an obvious bijection between the set of points $x \in \boldsymbol{H}_q$ satisfying $d(x, \boldsymbol{j}) = k$ and the set of points $y \in \boldsymbol{H}_q$ satisfying $d(y, a\boldsymbol{j} + b) = k$, given by

$$y = ax + b.$$

It is easy to see that this bijection is compatible with the identifications induced by the pseudometric d. Passing to the quotient space $\hat{\boldsymbol{H}}_q$, one obtains a bijection between the sets of points at a distance $\Delta = k$ from the points of $\hat{\boldsymbol{H}}_q$ obtained by the collapses of $\{-\boldsymbol{j}, \boldsymbol{j}\}$ and $\{-a\boldsymbol{j} + b, a\boldsymbol{j} + b\}$, respectively. This happens for every $a, b \in \boldsymbol{F}_q$, $a \neq 0$. The regularity of $V_0(q;k)$ is thus proved. Moreover, the 'behaviour at infinity' will be completely decided in what follows (see Proposition 3 below).

Definition. The 'length-spectrum' $\sum_q$ of $V(q)$ is defined to be the set of all possible values of k for which $V(q;k)$ is nonempty (i.e., it has at least one edge).

The structure of $\sum_q$ as a subset of $\{1, 2, \ldots, q\}$ is not at all obvious. One may be mislead by the representation (3) of the metric and think that every element of $\{1, 2, \ldots, q\}$ has the same good chance to appear as an element of the length spectrum. As we shall see, this is not true.

Let us suppose that $x = u + vj$ and $y = w + sj$ are two elements of $\boldsymbol{F}_{q^2}$, representing distinct elements of $V(q)$, say α, β, respectively. We will try to compute exactly some distances and to estimate some others, by using the formula (12), which gives d as a character sum. We distinguish two possibilities:

(A) $\alpha = \infty$, that is $v = 0$: This is the 'easy' situation, in the sense that it is not difficult to compute effectively the distance from ∞ to any other point of $V(q)$. All we need is to use the following exact estimate of the complete character sums with quadratic polynomial argument.

Theorem 2 (Lidl and Niederreiter [8, Ch. 5]). *Let $f(X) = a_2X^2 + a_1X + a_0 \in \boldsymbol{F}_q[X]$ with q odd and $a_0 \neq 0$. Let ψ be the quadratic character of $\boldsymbol{F}_q$, and $d = a_1^2 - 4a_0a_2$. If $d \neq 0$, then*

$$\sum_{c \in \boldsymbol{F}_q} \psi(f(c)) = -\psi(a_2).$$

If $d = 0$, then

$$\sum_{c \in \boldsymbol{F}_q} \psi(f(c)) = (q-1)\psi(a_2).$$

Using (12) together with Theorem 2, we obtain

$$\begin{aligned} \Delta(\infty, \beta) &= \frac{1}{2}\left[q - \sum_{a \in \boldsymbol{F}_q} \psi((y+a)(\bar{y}+a))\right] \\ &= \frac{1}{2}\left[q - \sum_{a \in \boldsymbol{F}_q} \psi(a^2 + aTr(y) + N(y))\right] \\ &= \frac{1}{2}\left[q + \psi(1)\right] = (q+1)/2. \end{aligned}$$

Corollary. *If $k \neq (q+1)/2$, then ∞ is an isolated vertex of $V(q;k)$, while for $k = (q+1)/2$, ∞ is joined by an edge with every other vertex, respectively. Consequently, the 'behaviour at infinity' of the associated graphs $V(q;k)$ is completely decided.*

(B) $\alpha, \beta \neq \infty$: In this case

$$\Delta(\alpha, \beta) = \frac{1}{2}\left[q - \sum_{a \in \boldsymbol{F}_q} \psi(P(a))\right],$$

where $P(X) = (X + x)(X + \bar{x})(X + y)(X + \bar{y})$ is a polynomial in $\boldsymbol{F}_q[X]$ which factors over $\boldsymbol{F}_q$ as a product of two distinct monic irreducible polynomials. The number of its distinct roots is $d = 4$ and, by Weil's theorem we get

$$\left| \Delta(\alpha, \beta) - \frac{q}{2} \right| \leqslant \frac{3}{2}\sqrt{q}\,.$$

This provides us with an asymptotic estimate of the length spectrum $\sum_q$. We summarize the above results in the following proposition which has a certain 'Riemann Hypothesis' flavour:

Proposition 3. (1) *The distance from* ∞ *to any other point of* $V(q)$ *is* $(q + 1)/2$. *In particular,* $(q + 1)/2 \in \sum_q$ *for every* q.

(2) *If* $k \in \sum_q$, *then*

$$\left| k - \frac{q}{2} \right| \leqslant \frac{3}{2}\sqrt{q}.$$

(3) *For every* $\varepsilon > 0$ *one can find* $M > 0$ *such that if* $q > M$, *and if the graph* $V(q; k)$ *is nonempty, then*

$$\frac{k}{q} \in \left(\frac{1}{2} - \varepsilon, \frac{1}{2} + \varepsilon \right).$$

Otherwise stated, the length spectrum accumulates, for large q, *in the middle part of the set* $\{1, 2, \ldots, q\}$.

(4) *All the graphs* $V_0(q; k)$ *are regular (possibly empty).*

As a corollary, for any fixed k, if q is large enough, $V(q; k)$ is empty. Notice that the graphs $X_q(g, a)$ [2], although defined in a similar way as ours $V(q; k)$'s, are always nonempty. They are $(q + 1)$-regular (see Section 1, or [2] for more details). The existence of a length spectrum is thus a feature of our model of finite upper half-plane.

Another interesting consequence would be the following: if we renormalize every $V(q)$ by dividing all the mutual distances by $q/2$, one can say that in the asymptotic limit these renormalized metric spaces approach a countably infinite metric space V with $d(x, y) = 1\ \forall x \neq y$. Thus, one can see these renormalized finite upper half-planes as 'small perturbations of complete graphs': all the mutual distances being in the range $1 + O(1/\sqrt{q})$. Finally, one could say, taking into account the way of defining the length spectrum, that $\sum_q$ plays the role of a 'parameter space' for the set of nonempty graphs $V(q; k)$.

6. Higher-dimensional generalization and further comments

One could try to define in a similar way high-dimensional analogues of the above 'plane construction'.

The characters of order two have the nice elementary property that $|a - b| = 1 - ab$ whenever a and b are two elements in their image. This basic fact made possible a 'safe' transition from the initial definition of the pseudometric d, given by (3), to the more elaborated (and useful) one (5), expressed as a character sum. That is the reason why the characters of order two seem to be more suitable for generalization.

The following heuristic principle will be our guide:

Often, a generalization starts with a new interpretation of the old facts.

So let us consider the action of the Frobenius automorphism $z \mapsto z^q$ on $\boldsymbol{F}_{q^2}$. The orbits with respect to this action are of two types. Namely, we have q orbits of cardinality 1, corresponding to the q elements of $\boldsymbol{F}_q$ fixed by Frobenius action. Then, the remaining $q^2 - q$ points are divided into $(q^2 - q)/2$ orbits of cardinality 2 each. The basic remark is that our finite upper half-plane $\boldsymbol{V}(q)$ is obtained out of the space of all Frobenius orbits described above, by identifying all the orbits of the first kind with a single point ∞. In the language of topology, $\boldsymbol{V}(q)$ is a quotient of the space of Frobenius orbits. The following remark presents in a more detailed way the space of all Frobenius orbits, in a general setting, relating it with the irreducible polynomials over $\boldsymbol{F}_q$:

Remark 2. Let $n \geqslant 2$ be a natural number, and $\Pi_n(q)$ the space of all the orbits of the Frobenius action on $\boldsymbol{F}_{q^n}/\boldsymbol{F}_q$. Also, for every natural number $d \geqslant 1$, define $\Phi_d(q)$ the set of all monic irreducible polynomials over $\boldsymbol{F}_q$, of degree d. Then there is a bijection between $\Pi_n(q)$ and

$$\bigcup_{d|n} \Phi_d(q)$$

which associates to every irreducible polynomial $f(X) \in \boldsymbol{F}_q[X]$ the set of all its roots (they are, of course, in $\boldsymbol{F}_{q^d}$, which we identify with a subfield of $\boldsymbol{F}_{q^n}$). Every orbit is thus identified with the zero-locus of sume monic irreducible polynomial over $\boldsymbol{F}_q$, of degree dividing n.

For example, if $n = 2$, the monic irreducible polynomials of degree 1 give us the q orbits of cardinal 1 which are the elements of $\boldsymbol{F}_q$, while the monic irreducibles of degree 2 give the remaining orbits of cardinal 2. The monic irreducible polynomial corresponding to the orbit

$$\{aj + b, -aj + b\}$$

is, obviously,

$$X^2 + 2bX + b^2 - ta^2$$

Let $n \geqslant 2$ be a natural number. Consider the following pseudometric on $\boldsymbol{F}_{q^n}$, which runs exactly as (3):

$$d(x,y) = \frac{1}{2} \sum_{a \in \boldsymbol{F}_q} |\chi(x+a) - \chi(y+a)|$$

$$= \frac{1}{2}\left[q - \sum_{a \in \boldsymbol{F}_q} \chi(x+a)\chi(y+a) \right], \tag{19}$$

where χ is the quadratic character of $\boldsymbol{F}_{q^n}$.

Remark 3. One easily checks that

$$d(x, \bar{x}) = 0$$

where $\bar{x} = x^q$ represents the Frobenius action. Thus every Frobenius orbit in $\boldsymbol{F}_{q^n}/\boldsymbol{F}_q$ is forced to collapse to a single point. However, the basic problem is whether we have any other identifications!

A relation similar to (9) holds in this general case. Now the norm is given by

$$N(z) = z^{1+q+q^2+\cdots+q^{n-1}}$$

for every z in $\boldsymbol{F}_{q^n}$. Suppose that $x \in \boldsymbol{F}_{q^n}$. Then we have the obvious polynomial identity

$$N(X+x) = P(X)^{n/e},$$

where $P(X)$ is the minimal polynomial of $-x$ over $\boldsymbol{F}_q$, e is its degree, and, of course,

$$N(X+x) = (X+x)(X+x^q)(X+x^{q^2}) \ldots (X+x^{q^{n-1}})$$

is the characteristic polynomial of $-x$ over $\boldsymbol{F}_q$.

Now, if $x, y \in \boldsymbol{F}_{q^n}$, $P(X)$, $Q(X) \in \boldsymbol{F}_q[X]$ are the minimal polynomials over $\boldsymbol{F}_q$ of $-x$, $-y$, respectively, with the corresponding degrees e and g, say, then one can rewrite (19), by using (9), as follows:

$$d(x,y) = \frac{1}{2}\left[q - \sum_{a \in \boldsymbol{F}_q} \psi(P(a)^{n/e} Q(a)^{n/g}) \right]. \tag{20}$$

Here ψ has the same meaning as before: it represents the quadratic character of $\boldsymbol{F}_q$, whose lift to $\boldsymbol{F}_{q^n}$ is χ.

Proposition 4. *The pseudometric* (19) *identifies the Frobenius orbits through* $x, y \in \boldsymbol{F}_{q^n}$ *whenever the numbers* n/e *and* n/g *are simultaneously even, where* e *and* g *represent the degrees of the minimal polynomials over* $\boldsymbol{F}_q$ *of the elements* x *and* y, *respectively.*

The proof comes at once if we look at the expression (20) of the pseudometric, while taking into account the fact that the degree of the minimal polynomial of x over $\boldsymbol{F}_q$ equals the degree of the minimal polynomial of $-x$.

Example. Take the case $n = 2$, and $x, y \in \boldsymbol{F}_q$. Then $e = g = 1$, while $n/e = n/g = 2$. We have seen that the pseudometric (3) forces us to identify x and y.

The following question appears now very natural: Does the pseudometric d given by (19) force any other identifications between various Frobenius orbits besides the ones prescribed by Proposition 4? Really, we have seen that in the case of the 'plane construction' we do not have any other identification.

Preserving the above notations, let us suppose that x and y represent two different Frobenius orbits, and that n/e and n/g are *not* both even. Then $-x$, $-y$ are also in distinct Frobenius orbits, their minimal polynomials, $P(X)$ and $Q(X)$, respectively, are distinct, and consequently the polynomial

$$H(X) = P(X)^{n/e} Q(X)^{n/g}$$

has $e + g$ distinct roots. Also it is easy to see that $H(X)$ is not, in this case, a square of some other polynomial.

All we need to is to apply now the Weil estimates (Theorem 1 above). We get

$$\left| \sum_{a \in \boldsymbol{F}_q} \psi(P(a)^{n/e} Q(a)^{n/g}) \right| \leqslant (e + g - 1)\sqrt{q} \tag{21}$$

As we have, obviously, $e, g \leqslant n$, we get, from (21)

$$\left| \sum_{a \in \boldsymbol{F}_q} \psi(P(a)^{n/e} Q(a)^{n/g}) \right| \leqslant (2n - 1)\sqrt{q}. \tag{22}$$

Now if one takes into account (20) and (22), it is clear that the Frobenius orbits through x and y are not identified provided that

$$q > (2n - 1)\sqrt{q}. \tag{23}$$

More exactly, two distinct Frobenius orbits of cardinalities e and g, respectivley, $e, g | n$, with at least one of the numbers n/e, n/g being odd, are *not* identified by the pseudometric (19) as long as $q > (e + g - 1)\sqrt{q}$, or, which is the same, as long as

$$q > (e + g - 1)^2. \tag{24}$$

Note that if both n/e and n/g are odd then

$$\psi(P(a)^{n/e} Q(a)^{n/g}) = \psi(P(a)Q(a)) \quad \forall a \in \boldsymbol{F}_q$$

while if, say, n/e is even and n/g is odd, then

$$\psi(P(a)^{n/e} Q(a)^{n/g}) = \psi(Q(a)) \quad \forall a \in \boldsymbol{F}_q$$

case in which, instead of (24) it is enough to require

$$q > (g - 1)^2 \tag{25}$$

in order to make sure that the Frobenius orbits through x and y are not identified by the pseudometric d.

After this brief discussion, one sees that (24) and (25) are sometimes sharper than (23). However, we also have to take into account the case in which $e = g = n$, so we cannot get rid of (23), at least by the present method. The general idea follows at once; if q is larger than a certain bound, which depends quadratically on n, then we do not have any other identifications besides the ones prescribed by Proposition 4. Consequently, we have the following general theorem:

Theorem 3. *Let $n \geqslant 2$ be a natural number, $q > (2n-1)^2$ an odd prime power and $V_n(q)$ be the quotient of the space $\Pi_n(q)$ of all Frobenius orbits of $\boldsymbol{F}_{q^n}/\boldsymbol{F}_q$, subjected to the following identification rule: two elements I, J, say, of $\Pi_n(q)$ are identified whenever the numbers $n/|I|$ and $n/|J|$ are both even. For $\alpha, \beta \in V_n(q)$, consider two representative Frobenius orbits $A, B \in \Pi_n(q)$, respectively, and two elements $x, y \in \boldsymbol{F}_{q^n}$, $x \in A$, $y \in B$. Then the function*

$$\Delta(\alpha, \beta) := d(x, y)$$

with d being given by (19), is well defined and represents a metric on $V_n(q)$. Moreover, the set $\Sigma_{n,q}$ of all possible distances between pairs of distinct points of $V_n(q)$ is subjected to the evaluation

$$\left| k - \frac{q}{2} \right| \leqslant \frac{2n-1}{2} \sqrt{q} \quad \forall k \in \Sigma_{n,q}.$$

The proof of the above result follows from our precedent discussion. The estimate on the length spectrum $\Sigma_{n,q}$ is an easy consequence of (20) and (22).

Corollary 1. *If n is odd and $q > (2n-1)^2$ then we do not need to perform any identification of $\Pi_n(q)$, and consequently $V_n(q) = \Pi_n(q)$: our 'upper half n-space' coincides with the space of all Frobenius orbits of $\boldsymbol{F}_{q^n}/\boldsymbol{F}_q$. For example, in the three-dimensional construction, the elements of $\boldsymbol{F}_q$ not only collapse, as in the case of the two-dimensional (plane) construction, but even remain distinct as elements of $V_3(q)$.*

At the other extreme, let us consider the case of 2-extensions, that is the case in which n is a power of 2.

Corollary 2. *If $n = 2^k$ and $q > (2n-1)^2$, then $V_n(q)$ is obtained out of $\Pi_n(q)$ by identifying any two Frobenius orbits which are both non-maximal (i.e., this is the case when both of them have less than 2^k elements). Consequently, the elements of $\boldsymbol{F}_{q^{n/2}}$ are all identified by the pseudometric d.*

Corollary 3. *Assume again $q > (2n-1)^2$, n even. Let $\boldsymbol{K}$ be the maximal 2-extension of $\boldsymbol{F}_q$ in $\boldsymbol{F}_{q^n}$, that is $\boldsymbol{K} = \boldsymbol{F}_{q^s}$, with s being the maximal power of 2 dividing n. Suppose that $x \in \boldsymbol{F}_{q^n}$ is such that its field $\boldsymbol{F}_q(x)$ contains $\boldsymbol{K}$. Then the Frobenius orbit through x is not subjected to any identification (by the pseudometric d) with some other Frobenius orbit. In the same time, all the elements of the field $\boldsymbol{F}_{q^{s/2}}$ collapse to a single point of $V_n(q)$.*

Notice that one can translate our discussion in terms of irreducible polynomials instead of using Frobenius orbits: this is possible by Remark 2.

One may note that in the higher-dimensional case there is not a point all of whose distances to the other points being expressed in a similar simple closed form as in the case of the '∞' point of the 'plane construction' (Proposition 3,(1)). The distances $\Delta(\alpha, \beta)$ in $V(q) = V_2(q)$ are easy to compute just because they are exponential sums for the Legendre character, with a quadratic polynomial argument.

We return now to our 'upper half-plane', in order to prove the existence of a nontrivial group of automorphisms.

It is easy to see that the functions

$$x \mapsto x + a \quad (a \in \boldsymbol{F}_q)$$

and

$$x \mapsto ax \quad (a \in \boldsymbol{F}_q^*)$$

are metric automorphisms of $V(q)$. Thus, we find that the group of all d-preserving maps of our upper half-plane contains a subgroup $\boldsymbol{A}(q)$ isomorphic to the group of all affine transformations of $\boldsymbol{F}_q$, viewed as an one-dimensional affine space (namely, of all non-constant linear functions $x \mapsto ax + b$, defined over $\boldsymbol{F}_q$, the group operation being the composition).

Consequently, we get a set of $q(q-1)$ isometries represented as above. If $k \in \sum_q$, then $\boldsymbol{A}(q)$ acts on $V(q;k)$.

To summarize, we defined a class of finite metric spaces $V(q)$, one for each odd prime power q. Structurally, they can be seen as 'finite upper half-planes', although the asymptotic behaviour is quite strange: for large q, $V(q)$ is, up to a distance renormalization, a 'small perturbation' of a complete graph with $1 + (q^2 - q)/2$ vertices (Proposition 3). Also we defined, in a way similar to [3], a class of graphs $V(q;k)$, $k \in \sum_q$, parametrized by the 'length-spectrum $\sum_q$. The combinatorial structure of the graphs $V(q;k)$ seems to be rich, as the cases $q = 3$, $q = 5$, $q = 7$ suggest. An additional reason to believe this is the regularity of the 'finite parts' $V_0(q;k)$ of the graphs $V(q;k)$. Moreover, we determined precisely the 'behaviour at infinity' of each one of the associated graphs. However, we think that some larger scale computer search would be helpful.

Finally, we managed to extend the plane construction to higher-dimensional case, in which, provided that q is large enough (the specific constraint in dimension n is $q > (2n-1)^2$, then a similar construction works, which produces higher-dimensional analogues $V_n(q)$ of $V(q)$. The finite metric spaces $V_n(q)$ can be obtained out of the corresponding spaces $\Pi_n(q)$ of Frobenius orbits of $\boldsymbol{F}_{q^n}/\boldsymbol{F}_q$, by making appropriate identifications (Theorem 3). Concerning the length-spectrum, its higher-dimensional behaviour is quite similar with the two dimensional one: the generic distance in $V_n(q)$ can be expressed as

$$\frac{q}{2} + O(\sqrt{q})$$

where the constant implied by 'O' can be chosen $n - 1/2$ in the n-dimensional case.

Acknowledgements

The author wishes to thank the referee for the enlightening comments and suggestions. The same warmest thanks are due to Professors George Andrews and Leonid Vaserstein, for their constant help and support.

References

[1] J. Angel, N. Celniker, S. Poulos, A. Terras, C. Trimble and E. Velasquez, Special functions on finite upper half-planes, Contemp. Math. 138 (1992) 1–26.
[2] J. Angel, S. Poulos, A. Terras, C. Trimble and E. Velasquez, Spherical functions and transforms on finite upper half planes: eigenvalues of the combinatorial laplacian, uncertainty, traces, preprint.
[3] E. Bombieri, Counting points on curves over finite fields (d'apres Stepanov), Sem. Bourbaki 1972/1973, Exp. 430, Lecture Notes in Math., Vol. 383 (Springer, Berlin, 1974) 234–241.
[4] N. Celniker, S. Poulos, A. Terras, C. Trimble and E. Velasquez, Is there life on finite upper half planes?, Comtemp. Math. 143 (1993) 65–88.
[5] H. Davenport, On primitive roots in finite fields, Quart. J. Math. (2) 8 (1937) 308–312.
[6] M. Deuring, Lectures on the theory of algebraic functions of one variable, Lecture Notes in Math., Vol. 314 (Springer, Berlin, 1973).
[7] H. Hasse, Theorie der relativ-zyklischen algebraichen Functionenkorper, insbesondere bei endlichen Konstantenkorper, J. Reine Angew. Math. 172 (1934) 37–54.
[8] R. Lidl and H. Niederreiter, Finite fields, in: Encyclopedia of Mathematics and its applications, Vol. 20 (Addison-Wesley, Reading MA, 1983).
[9] W. Schmidt, Equations over finite fields, an elementary approach, Lecture Notes in Math., Vol. 536 (Springer, Berlin, 1976).
[10] H. Stichtenoth, Algebraic Function Fields and Codes (Springer, Berlin, 1993).
[11] M. Tsfasman and S. Vladut, Algebraic-geometric codes, in: Math. and its Appl. (Kluwer Acad. Publishers, Dordrecht, 1991).
[12] A. Weil, Sur les courbes algebriques et les varietes qui s'en deduisent, Actualites Sci. Ind., No. 1041 (Hermann, Paris, 1948).